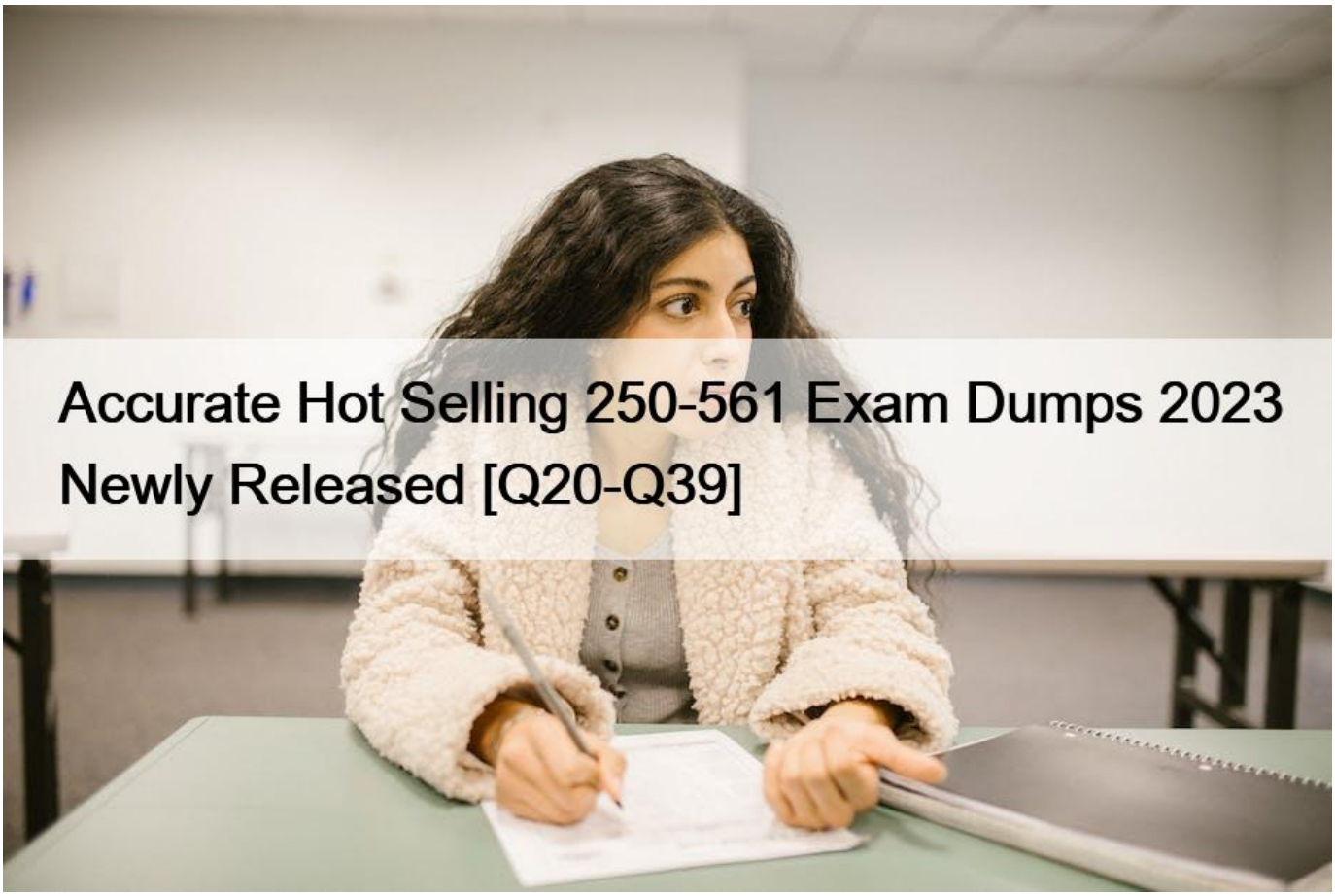
Accurate Hot Selling 250-561 Exam Dumps 2023 Newly Released [Q20-Q39



Accurate Hot Selling 250-561 Exam Dumps 2023 Newly Released
Get 100% Authentic Symantec 250-561 Dumps with Correct Answers

QUESTION 20

Which IPS Signature type is Primarily used to identify specific unwanted traffic?
* Attack
* Probe
* Audit
* Malcode

QUESTION 21

What is the primary issue pertaining to managing roaming users while utilizing an on-premise solution?
* The endpoint is missing timely policy update
* The endpoint is absent of the management console
* The endpoint fails to receive content update
* The endpoint is more exposed to threats

QUESTION 22

What does SES’s advanced search feature provide when an administrator searches for a specific term?
* A search modifier dialog
* A search wizard dialog
* A suggested terms dialog
* A search summary dialog

QUESTION 23

Files are blocked by hash in the blacklist policy.

Which algorithm is supported, in addition to MD5?
* SHA256
* SHA256 “salted”
* MD5 “Salted”
* SHA2

QUESTION 24

An administrator suspects that several computers have become part of a botnet. What should the administrator do to detect botnet activity on the network?
* Enable the Command and Control Server Firewall
* Add botnet related signatures to the IPS policy’s Audit Signatures list
* Enable the IPS policy’s Show notification on the device setting
* Set the Antimalware policy’s Monitoring Level to 4

QUESTION 25

An administrator selects the Discovered Items list in the ICDm to investigate a recent surge in suspicious file activity. What should an administrator do to display only high risk files?
* Apply a list control
* Apply a search rule
* Apply a list filter
* Apply a search modifier

QUESTION 26

Which two (2) steps should an administrator take to guard against re-occurring threats? (Select two)
* Confirm that daily active and weekly full scans take place on all endpoints
* Verify that all endpoints receive scheduled Live-Update content
* Use Power Eraser to clean endpoint Windows registries
* Add endpoints to a high security group and assign a restrictive Antimalware policy to the group
* Quarantine affected endpoints

QUESTION 27

Which antimalware intensity level is defined by the following: “Blocks files that are most certainly bad or potentially bad files. Results in a comparable number of false positives and false negatives.”

* Level 5
* Level 2
* Level 1
* Level 6

QUESTION 28

Which report template type should an administrator utilize to create a daily summary of network threats detected?
* Network Risk Report
* Blocked Threats Report
* Intrusion Prevention Report
* Access Violation Report

QUESTION 29

Which Anti-malware technology should an administrator utilize to expose the malicious nature of a file created with a custom packet?
* Sandbox
* SONAR
* Reputation
* Emulator

QUESTION 30

Which report template includes a summary of risk distribution by devices, users, and groups?
* Device Integrity
* Threat Distribution
* Comprehensive
* Weekly

QUESTION 31

Which communication method is utilized within SES to achieve real-time management?
* Heartbeat
* Standard polling
* Push Notification
* Long polling

QUESTION 32

Which term or expression is utilized when adversaries leverage existing tools in the environment?
* opportunistic attack
* script kiddies
* living off the land
* file-less attack

QUESTION 33

What must an administrator check prior to enrolling an on-prem SEPM infrastructure into the cloud?
* Clients are running SEP 14.2 or later

* Clients are running SEP 14.1.0 or later
* Clients are running SEP 12-6 or later
* Clients are running SEP 14.0.1 or late

QUESTION 34

Which option should an administrator utilize to temporarily or permanently block a file?
* Delete
* Hide
* Encrypt
* Blacklist

QUESTION 35

What happens when an administrator blacklists a file?
* The file is assigned to the Blacklist task list
* The file is automatically quarantined
* The file is assigned to a chosen Blacklist policy
* The file is assigned to the default Blacklist policy

QUESTION 36

After editing and saving a policy, an administrator is prompted with the option to apply the edited policy to any assigned device groups.

What happens to the new version of the policy if the administrator declines the option to apply it?
* The policy display is returned to edit mode
* The new version of the policy is deleted
* An unassigned version of the policy is created
* The new version of the policy is added to the “in progress” list

QUESTION 37

Which two (2) skill areas are critical to the success of incident Response Teams (Select two)
* Project Management
* Incident Management
* Cyber Intelligence
* Incident Response
* Threat Analysis

QUESTION 38

Which two (2) Discovery and Deploy features could an administrator use to enroll MAC endpoints? (Select two)
* Push Enroll
* A custom Installation package creator pact
* A default Direct Installation package
* Invite User
* A custom Direct installation package

QUESTION 39

Which two (2) options is an administrator able to use to prevent a file from being fasely detected (Select two)

* Assign the file a SHA-256 cryptographic hash
* Add the file to a Whitelist policy
* Reduce the Intensive Protection setting of the Antimalware policy
* Register the file with Symantec’s False Positive database
* Rename the file

Dumps of 250-561 Cover all the requirements of the Real Exam: https://www.dumpleader.com/250-561_exam.html]